In the Claims:

Please amend claims 1 and 3-8. Please add new claims 13-21. The claims are as follows:

1. (Currently amended) A method enabling a network-addressable device to detect use of its identity by a spoofer, comprising the acts of:

receiving a message by the network-addressable device;

detecting a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative ~~of activity~~ of a denial of service attack on a target by a spoofing vandal using an identity of the network-addressable device; and

generating a spoofing alert responsive to the act of detecting the communication protocol violation.

2. (Original) A method enabling a network-addressable device to detect use of its identity by a spoofer, comprising the acts of:

receiving a message by the network-addressable device;

detecting a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of activity of a spoofing vandal using the identity of the network-addressable device in an attack on a target;

recording attributes of the message;

advancing the value of a counter associated with the target;

comparing the value of the counter with a predetermined threshold; and

generating a spoofing alert when the value of the counter exceeds the threshold.

PAGE 3/13 * RCVD AT 12/27/2004 12:18:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-10

3. (Currently amended) The method of claim 2, ~~further comprising the act of sending the spoofing alert to a network administrator~~ wherein the network-addressable device is connected to the target by a communication network.

4. (Currently amended) The method of claim 3, ~~wherein the~~ further comprising sending the spoofing alert to a network administrator who is ~~associated with~~ responsible for the network-addressable device.

5. (Currently amended) The method of claim 3, ~~wherein the~~ further comprising sending the spoofing alert to a network administrator who is ~~associated with~~ responsible for the target.

6. (Currently amended) The method of claim [[2]] 3, further comprising ~~the act of~~ blocking the message from advancing further into the network-addressable device.

7. (Currently amended) The method of claim [[2]] 3, wherein ~~the act of~~ said recording comprises recording said attributes of the message ~~includes the act of writing a record to~~ in a spoofing logbook database.

8. (Currently amended) The method of claim [[2]] 7, wherein ~~the act of recording attributes of the message includes the act of writing the message to a spoofing logbook database~~ said recorded attributes of the message in the spoofing logbook database comprise a source address of the message, an indication of a nature of the activity of the spoofing vandal, and a time at which the

PAGE 4/13 * RCVD AT 12/27/2004 12:18:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-10

message has been received.

9. (Original) The method of claim 2, wherein the identity of the network-addressable device is a TCP/IP source address of the network-addressable device.

10. (Original) The method of claim 2, wherein the protocol violation includes reception by the network-addressable device of an unsolicited response message sent by the target.

11. (Original) The method of claim 2, wherein the protocol violation includes the reception by the network-addressable device of an ICMP reply sent by the target when an ICMP PING has not been sent to the target by the network-addressable device.

12. (Original) The method of claim 2, wherein the protocol violation includes reception by the network-addressable device of a SYN/ACK message when a SYN message has not been sent to the target by the network-addressable device.

13. (New) The method of claim 3, wherein the communication network comprises the Internet.

14. (New) The method of claim 3, wherein the attack on the target by the spoofing vandal comprises a denial of service attack on the target by the spoofing vandal.

15. (New) The method of claim 3, further comprising providing a first network administrator

PAGE 5/13 * RCVD AT 12/27/2004 12:18:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-10

who is responsible for the network-addressable device and a second network administrator who is responsible for the target.

16. (New) The method of claim 15, further comprising sending the spoofing alert to both the first network administrator and the second network administrator.

17. (New) The method of claim 15, wherein the first network administrator is a first automated network management system, and wherein the second network administrator is a second automated network management system.

18. (New) The method of claim 3, wherein the network-addressable device is connected to the spoofing vandal by the communication network.

19. (New) The method of claim 3, wherein said detecting, recording, advancing, comparing, and generating are performed by the network-addressable device.

20. (New) The method of claim 2, wherein the network-addressable device is connected to the spoofing vandal by a communication network.

21. (New) The method of claim 2, wherein said detecting, recording, advancing, comparing, and generating are performed by the network-addressable device.

PAGE 6/13 * RCVD AT 12/27/2004 12:18:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID: * DURATION (mm-ss):03-10